**УТВЕРЖДАЮ**

Директор
ГКУ ТО «ЦИТТО»

_____Усманов А.Р.

«___» _____ 2021 г.

# РЕГЛАМЕНТ ПОДКЛЮЧЕНИЯ К ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В СФЕРЕ ЗДРАВООХРАНЕНИЯ ТЮМЕНСКОЙ ОБЛАСТИ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

2021

## 1. Термины и определения

**ГИСЗ ТО** - Государственная информационная система в сфере здравоохранения Тюменской области.

**ГИС УРМО ТО** - Государственная информационная система управления ресурсами медицинских организаций Тюменской области.

**ГКУ ТО «ЦИТТО»** - Государственное казенное учреждение «Центр информационных технологий Тюменской области».

**ЗСПД** - Защищенная сеть передачи данных ГИС УРМО ТО.

**ИБ** - Информационная безопасность.

**ЛВС** - Локальная вычислительная сеть.

**УИВ** - Участник информационного взаимодействия.

**ИС УИВ** - Информационная система участник информационного взаимодействия.

**ПАК** - Программно-аппаратный комплекс.

**СКЗИ** - Средства криптографической защиты информации (программные и программно-аппаратные).

**ФСБ** - Федеральная служба безопасности Российской Федерации

**ФСТЭК** - Федеральная служба по техническому и экспортному контролю

**ЦОД ПТО** - Центр обработки данных Правительства Тюменской области (основная и резервная площадки).

**ИС УИВ** - Информационные системы Участника информационного взаимодействия

**Администратор безопасности УИВ** - Лицо, отвечающее за организационные вопросы, возникающие при подключении к ЗСПД со стороны УИВ.

**Администратор ИБ** - Администратор информационной безопасности ЗСПД ГИСЗ ТО.

## 2. Общие положения

### 2.1. Предмет регулирования

Настоящий Регламент определяет порядок подключения участников информационного взаимодействия к защищенной сети передачи данных ViPNet ГИС УРМО ТО, являющейся компонентом ГИСЗ ТО.

Актуальная версия Регламента размещена на официальном сайте ГКУ ТО ЦИТТО в разделе «Главная» - «Направление деятельности» - «Государственная информационная система в сфере здравоохранения Тюменской области» - «Нормативно-правовая информация».

### 2.2. Общие сведения о ГИС УРМО ТО

ГИС УРМО ТО соответствует требованиям безопасности информации, предъявляемым к государственным информационным системам 2 класса защищенности, в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», 2 уровню защищенности персональных данных в соответствии с постановлением

Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Оператором ГИС УРМО ТО является ГКУ ТО "ЦИТТО"(далее — Оператор).

Лицом, обрабатывающим информацию и эксплуатирующим ГИС УРМО ТО являются Медицинские учреждения Тюменской области.

### 2.3. Участники информационного взаимодействия

Участниками информационного взаимодействия являются:

- Оператор ГИС УРМО ТО;
- Медицинские организации частной системы здравоохранения;
- Медицинские организации Тюменской области.

### 2.4. Нормативно-правовые акты

Настоящий Регламент разработан во исполнение требований следующих нормативно-правовых и локальных нормативных актов:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утверждены приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378;
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утверждена приказом Федерального агентства правительственной связи и информации от 13.06.2001 № 152;
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005, утверждено приказом Федеральной службы безопасности Российской Федерации от09.02.2005 г. № 66).

### 2.5. Сведения о защищенной сети

Информационное взаимодействие ГИС УРМО ТО с участниками информационного взаимодействия осуществляется с использованием СКЗИ, сертифицированных ФСБ по классу не ниже «КС2», совместимых с технологией ViPNet.

### 2.6. Условия подключения к ЗСПД

В настоящем пункте приведены сведения об условиях подключения к ЗСПД участников информационного взаимодействия с подсистемами ГИСЗ. Описанные в настоящем разделе условия являются обязательными для начала работ по подключению к ЗСПД.

ИС УИВ, подключаемая к ЗСПД, должна иметь подтверждение выполнения требований о защите информации, обрабатываемой в ИС УИВ, в том числе полученной из ГИС УРМО ТО (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения), в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах не ниже 2 класса защищенности, установленными Федеральной службой по техническому и экспортному контролю в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», требованиями к защите персональных данных при их обработке в информационных системах персональных данных, установленными Правительством Российской Федерации в соответствии с пунктом 2 части 3 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и требованиями раздела II приказа Минздрава России от 24 декабря 2018 года №911н.

## 3. Варианты подключения к ЗСПД

В целях реализации информационного взаимодействия с ГИС УРМО ТО УИВ выбирает один из следующих вариантов подключения к защищенной сети передачи данных ГИС УРМО ТО в зависимости от количества пользователей, используемых операционных систем.

### 3.1. Вариант 1 - Подключение ИС расположенной в защищенном сегменте сети УИВ

Подключение ИС расположенной в защищенном сегменте сети УИВ к защищенной сети ViPNet ГИС УРМО ТО обеспечивается через программно-аппаратный комплекс ViPNet Coordinator HW 4, сертифицированный ФСБ по классу не ниже КС2.

Для подключаемой ИС УИВ должны быть выполнены требования, указанные в п. 2.6 Регламента. В таком случае УИВ принимает на себя обязательство по обеспечению технической поддержки купленного устройства.

### 3.2. Вариант 2 — Межсетевое взаимодействие

Данный вариант применим в случае необходимости организации межсетевого взаимодействия существующих сетей VipNet УИВ с защищенной сетью ГИС УРМО ТО.

Подключаемые сети ViPNet должны быть по классу не ниже КС2. Для подключаемой ИС УИВ должны быть выполнены требования, указанные в п. 2.6 Регламента.

### 3.3. Вариант 3 — Клиентский доступ

Данный Вариант применим в случае необходимости клиентского доступа к ГИС УРМО ТО. Подключение АРМ к ГИС УРМО ТО обеспечивается через программное обеспечение ViPNet Client 4.x, сертифицированное ФСБ по классу не ниже КС2.

Для подключаемой ИС УИВ должны быть выполнены требования, указанные в п. 2.6 Регламента. В таком случае УИВ принимает на себя обязательство по обеспечению технической поддержки эксплуатируемого УИВ программного обеспечения ViPNet Client 4.x.

## 4. Порядок подключения к защищенной сети ГИС УРМО ТО

Подключение участников информационного взаимодействия в части к ЗСПД ГИС УРМО ТО осуществляется в следующем порядке:

1. Заявитель выбирает приемлемую схему подключения к ЗСПД ГИС УРМО ТО (см. Раздел 2 настоящего Регламента);
2. Заявитель осуществляет закупку необходимого программного обеспечения или программно-аппаратного комплекса для подключения к ЗСПД УРМО ТО;
3. Заявитель направляет в адрес Оператора заполненную заявку на подключение к ЗСПД ГИС УРМО ТО;

**Заявка на подключение включает в себя:*

- *официальное письмо на имя руководителя Оператора;*
- *заполненная анкета на подключение;*
- *копия приказа о назначении ответственного за эксплуатацию СКЗИ.*

4. Оператор проводит оценку выполнения требований, предъявляемых к подключаемой ИС УИВ и технической возможности подключения к ЗСПД УРМО ТО и в течении 10 рабочих дней, направляет в адрес заявителя принятое решение.

Оператор вправе отказать заявителю в подключении к защищенной сети ГИС УРМО ТО. Возможными причинами отказа в подключении к защищенной сети ГИС УРМО ТО могут являться:

**а)** запрашиваемые сведения предоставлены не в полном объеме;

**б)** класс используемых средств криптографической защиты информации ниже КС2;

**в)** ИС УИВ не соответствует требованиям по обеспечению безопасности обрабатываемой информации, предъявляемым к ИС не ниже 2 класса защищенности(отсутствует аттестат соответствия требованиям по безопасности информации или иное подтверждение такого соответствия).

В случае положительного решения о подключении заявителя к ЗСПД УРМО ТО:

- для варианта 1 и 3 подключения:

1. Оператор проводит формирование файла ключевого дистрибутива (DST) и направляет ключевую информацию заявителю доверенным способом передачи;
2. Заявитель проводит работы по инициализации ViPNet узла с использованием файла ключевого дистрибутива (DST).;
3. Администратор ИБ проверяет доступность узла сети.

- для варианта 2 подключения:

1. Администратор ИБ и администратор сторонней сети ViPNet УИВ согласовывают время проведения работ;
2. Администратор ИБ осуществляет формирование файла с межсетевой информацией и индивидуального симметричного межсетевого мастер-ключа (далее – мастер-ключ);
3. Администратор ИБ доверенным способом передает экспортные файлы администратору сторонней сети ViPNet УИВ;
4. Администратор сторонней сети ViPNet УИВ принимает межсетевую информацию, импортирует мастер-ключ,создает файл с ответной межсетевой информацией и передает администратору ИБ;
5. Администратор ИБ проверяет доступность узла сети;
6. При успешной проверке заявитель направляет Оператору подписанный протокол согласно Приложению № 2 в срок не превышающий 5 рабочих дней.

## 5. Политика обеспечения информационной безопасности

Для информационных систем УИВ, подключаемых к ЗСПД УРМО ТО , должны выполняться требования, предъявляемые нормативно-правовыми актами Российской Федерации в области защиты информации к обеспечению не ниже 2 уровня защищенности персональных данных, и к обеспечению защищенности государственных информационных систем не ниже класса К2.

К организационным мерам защиты информации относятся:

– разработка и утверждение организационно-распорядительной документации;

– контроль доступа;

– ведение журналов учета СКЗИ.

– К техническим мерам защиты информации относятся:

– применение лицензионных операционных систем(либо сертифицированных операционных систем) с актуальными пакетами обновлений;

– применение сертифицированных средств антивирусной защиты;

– применение сертифицированных средств защиты информации от несанкционированного доступа;

– применение сертифицированных средств межсетевого экранирования;

– применение сертифицированных средств криптографической защиты.

## 6. История изменений

| № п/п | Версия, дата документа | Автор | Примечания |
|---|---|---|---|
| | v.1 | Аникин А.Н. | Введен впервые |
| | | | |
| | | | |

Приложение № 1

# Анкета на подключение к ЗСПД ГИС УРМО ТО

## 1. Общие сведения об УИВ

| | | |
|---|---|---|
| **1.** | Полное наименование организации | |
| **2.** | Сокращенное наименование организации | |
| **3.** | ИНН | |
| **4.** | ОГРН | |
| **5.** | Юридический адрес организации | |
| **6.** | Фактический (почтовый) адрес организации | |
| **7.** | Телефон организации | |
| **8.** | ФИО сотрудника (администратора ИБ УИВ) | |
| **9.** | Контактный телефон (администратора ИБ УИВ) | |
| **10.** | Контактная электронная почта (администратора ИБ УИВ) | |

## 2. Сведения об имеющихся у УИВ средствах для подключения к СЗПД ГИС УРМО ТО

| | | |
|---|---|---|
| **11.** | Планируемый вариант подключения к ЗСПД в соответствии с разделом 2 Регламента(Вариант1, Вариант2, Вариант3) | |
| **12.** | Модель ViPNet Coordinator | |
| **13.** | Количество ViPNet Coordinator | |
| **14.** | Класс криптографической защиты ViPNetCoordinator (КС1, КС2, КС3) | |
| **15.** | Номер сторонней сети ViPNet *(только для Варианта 2)* | |
| **16.** | Класс защищенности сторонней сети ViPNet *(только для Варианта 2)* | |

**3. Сведения о информационной системе УИВ**

| | | |
|---|---|---|
| **17.** | Наименование информационной системы | |
| **18.** | Класс защищенности в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации,не составляющей государственную тайну,содержащейся в государственных информационных системах» | |
| **19.** | Уровень защищенности персональных данных в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» | |
| **20.** | Сведения соответствия информационной системы (подключаемого сегмента информационной системы), требованиям по безопасности информации (номер аттестата соответствия или иного подтверждающего документа, дата выдачи, срок действия) | |

**4. Сведения о пользователях, допущенных к работе с СКЗИ (администратор ИБ)**

| № | ФИО | Должность | Электронная почта | Контактный телефон | Номер приказа о допуске к работе с СКЗИ |
|---|---|---|---|---|---|
| | | | | | |

Приложение № 2

**Форма протокола установления межсетевого взаимодействия**

1. Межсетевое взаимодействие устанавливается между следующими сетями ViPNet:

| **Номер сети VipNet** | **Наимерование владельца сети VipNet, ОГРН** | **Наименование пользователя сети ViPNet, ОГРН** |
|---|---|---|

2. Передача начального и ответного экспорта между сетями № _____ и №_____ осуществлялась через специалиста, уполномоченного на данные действия.

3. При установлении межсетевого взаимодействия были произведены импорты справочников главных абонентов сети.

4. Смена межсетевых ключей, изменение состава АП, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] [Деловая почта] с указанием производимых изменений.

5. Стороны обязуются без предварительного согласия не производить изменений в настройках и структуре защищенных сетей ViPNet, которые могут привести к нарушению межсетевого взаимодействия.

Администратор информационной безопасности ЗСПД УРМО ТО

_____/_____

подпись ФИО

«____» _____20___

Администратор информационной безопасности защищенной сети УИВ

_____/_____

подпись ФИО

«____» _____20___